

**Operational, Support Processes, & Procedures Manual** rectangle

**AWS CyberShift Initiative**

Date Prepared: 29th of June, 2023

**Contents Page**

[**Start-up & Shutdown Procedures: 2**](#_gjdgxs)

[Operating Systems 2](#_y2na05svqesb)

[Windows Server: 2](#_y2na05svqesb)

[Linux Web Server: 3](#_ggd6ugdd7p1o)

[**Start-up & Shutdown Procedures for Security Software: 3**](#_fz4mk9i7ligs)

[Firewalls 3](#_y2na05svqesb)

[IPD/IDS 5](#_h4drftyouuhn)

[Anti-virus/Malware 6](#_ifmbjl5pgzan)

[Log Monitoring and Analysis 9](#_by2vlcczk3n2)

[Real-time Monitoring 10](#_66plshqhnhcz)

[**Regular Maintenance Activities with Schedule: 11**](#_9l63tfbbwovv)

[Windows AD Server 11](#_c0rllqtxw5a8)

[Linux Web Server 11](#_fh1plkkdthtl)

[**Support Processes and Documentation 11**](#_6dxgz9y6ao6)

[**User Access Management: 12**](#_xhq4o1drbfk6)

[Processes of Access Management 12](#_bgmxjghlrunf)

[Managing User Accounts 12](#_n3gt088h7ogq)

[**Support Contacts: 13**](#_d913f2hljihy)

|  |
| --- |
| Start-up & Shutdown Procedures: |

|  |  |
| --- | --- |
| Operating Systems | |
| Windows Server: | **Start-up**:   1. Power on the server by pressing the power button. 2. Wait for the Windows Server operating system to load. This process may take a few minutes. 3. Once the login screen appears, enter the appropriate administrative credentials 4. Click "**Sign in**" or press **Enter** to log in. 5. After logging in, the desktop environment will load, and you can start using the server. 6. Verify that all necessary services and applications are running as expected 7. In the **‘Start’** menu, start the windows server by opening the **‘Server Manager’** 8. Once the Server Manager dashboard opens, inspect the dashboard for any alerts requiring attention, and resolve the issues (if any) |
| **Shutdown**:   1. Save and close any open applications or services. 2. Click on the "**Start**" button located at the bottom left corner of the screen. 3. In the Start menu, click on the power button icon. 4. A submenu will appear with options like **Shutdown**, **Restart**, **Sleep**, or **Hibernate**. 5. Select "**Shutdown**" to power off the server gracefully. 6. If there are any unsaved changes or running processes, you may be prompted to save or close them. 7. Confirm the action by clicking "**Shutdown**" or pressing Enter. 8. Wait for the server to complete the shutdown process. It will automatically close running programs and services before powering off. 9. Once the server has shut down, it is safe to turn off the power. |
| Linux Web Server: | **Start-up**:   1. Power on the server by pressing the power button. 2. Wait for the Linux operating system to load. This process may vary depending on the distribution and server hardware. 3. Once the login prompt appears in the terminal or the graphical login screen is displayed, enter the appropriate administrative credentials (username and password). 4. Press Enter to log in. 5. After logging in, the command-line interface or desktop environment will be accessible. 6. Verify that all necessary services and applications are running as expected, and if required, the Apache web server status can be checked by typing the following command: sudo systemctl status apache2 |
| **Shutdown**:   1. Save and close any open applications or services. 2. Open a terminal by navigating to the Applications menu or using the keyboard shortcut (e.g., Ctrl+Alt+T). 3. In the terminal, type the following command and press Enter: sudo shutdown -h now 4. If prompted, enter the administrator password. 5. Confirm the action by typing "**y**" or "**yes**" and press Enter. 6. The Linux server will initiate the shutdown process. It will notify logged-in users and begin terminating running processes. 7. Wait for the system to complete the shutdown process. It will halt all processes and services before powering off. 8. Once the server has shut down, it is safe to turn off the power |

|  |
| --- |
| Start-up & Shutdown Procedures for Security Software: |

|  |  |
| --- | --- |
| Firewalls | |
| **pfSense (Windows Server)** | To **start** the pfSense firewall in a Hyper-V environment on Azure   1. Open a web browser and navigate to the Azure Management Portal (portal.azure.com). 2. Enter your credentials to log in to the Azure Management Portal. 3. In the Azure Management Portal, locate and click on "Virtual Machines" in the left-hand menu. 4. From the list of virtual machines, identify the VM running pfSense and click on it to select it. 5. In the pfSense VM's overview page, locate and click on the "Start" button to initiate the VM's startup process. 6. Once the VM start command is issued, the Azure platform will begin booting the pfSense VM. You can monitor the startup progress through the Azure portal. It may take a few minutes for the VM to fully start and be accessible. 7. After the pfSense VM has started successfully, you can access its web-based management interface to configure and manage the firewall.  **Follow these steps:**   **a**. Open a web browser on your local machine or any computer connected to the same network.  **b**. Enter the IP address “**192.168.1.1**” of the pfSense VM in the address bar of the web browser.  **c.** The pfSense login page should appear. Enter the appropriate credentials to log in to the pfSense firewall.   1. Once you have logged in to the pfSense firewall interface, you can verify its operation and ensure that the necessary configurations and rules are in place to protect the Windows 2022 AD Server and other network resources |
| To properly **shut down** the pfSense firewall in a Hyper-V environment on Azure   1. Open a web browser and navigate to the Azure Management Portal (portal.azure.com). 2. Enter your credentials to log in to the Azure Management Portal. 3. In the Azure Management Portal, locate and click on "Virtual Machines" in the left-hand menu. 4. From the list of virtual machines, identify the VM running pfSense and click on it to select it. 5. In the pfSense VM's overview page, locate and click on the "Stop" button to initiate the VM's shutdown process. 6. A confirmation dialog will appear asking you to confirm the shutdown action. Review the information and click "Yes" to proceed with the shutdown. 7. The Azure platform will initiate the shutdown process for the pfSense VM. It may take a few moments for the VM to fully stop. You can monitor the progress through the Azure portal. 8. Once the VM has stopped successfully, you will see its status change to "Stopped" in the Azure portal. |
| **Sophos Firewall (Linux Web Server)** | To **start** the Sophos firewall in a Hyper-V environment on Azure:   1. Open a web browser and navigate to the Azure Management Portal ([portal.azure.com](https://azure.microsoft.com/en-us/get-started/azure-portal)). 2. Enter your credentials to log in to the Azure Management Portal. 3. In the Azure Management Portal, navigate to the Virtual Machines section and locate the virtual machine running the Sophos firewall. 4. Select the Sophos firewall VM from the list, and click on the "**Start**" button in the toolbar to initiate the startup process. 5. Once the VM start command is issued, the Azure platform will begin booting the Sophos firewall VM. You can monitor the startup progress through the Azure portal. It may take a few minutes for the VM to fully start and become accessible. 6. After the Sophos firewall VM has started successfully, you can access its management interface to configure and manage the firewall.   **Follow these steps:**  **a.** Open a web browser on your local machine or any computer connected to the same network.  **b.** Enter the IP address and port number of the Sophos firewall in the address bar of the web browser. In this case, enter "**192.168.2.100:4444**"  **c.** The Sophos firewall management interface should appear.  Follow any on-screen instructions to log in to the interface.   1. Once you have logged in to the Sophos firewall management interface, you can verify its operation and ensure that the necessary configurations and rules are in place to protect the Linux 2 web server and other network resources. |
| To properly **shut down** the Sophos firewall in a Hyper-V environment on Azure:   1. Open a web browser and navigate to the Azure Management Portal ([portal.azure.com](https://azure.microsoft.com/en-us/get-started/azure-portal)). 2. Enter your credentials to log in to the Azure Management Portal. 3. In the Azure Management Portal, navigate to the Virtual Machines section and locate the virtual machine running the Sophos firewall. 4. Select the Sophos firewall VM from the list, and click on the "**Stop**" button in the toolbar to initiate the shutdown process. 5. A confirmation dialog will appear asking you to confirm the shutdown action. Review the information and click "**Yes**" to proceed with the shutdown. 6. The Azure platform will initiate the shutdown process for the Sophos firewall VM. It may take a few moments for the VM to fully stop. You can monitor the progress through the Azure portal. 7. Once the VM has stopped successfully, you will see its status change to "**Stopped**" in the Azure portal. |

|  |  |
| --- | --- |
| IPD/IDS | |
| **Snort (Windows Server)** | **Start-up**:   1. Ensure the windows server is on and operating as expected. 2. To start Snort, open a command prompt window (cmd.exe) with administrative privileges. To start Snort, you need to execute the Snort binary with specific command-line options 3. Navigate to the Snort installation directory in the command prompt window ( cd C:\Snort\bin 4. Run the following command to start Snort: snort -i 192.168.0.0 -c C:\sort\etc\ snort.conf 5. Snort will start running and begin analyzing network traffic based on your configured rules 6. Snort will generate output based on the detected network activity. These Log files can be seen in the following directory C:\snort\log |
| **Shutdown**:   1. Locate the Snort console window that is currently running. 2. Press Ctrl+C in the Snort console window. This sends a termination signal to Snort, and it should gracefully shut down. 3. After executing the termination command, the Snort console window should close, indicating that Snort has successfully shut down. |
| **Snort (Linux Web Server)** | **Start-up**:   1. Open a terminal on your Linux system 2. Run Snort with the command-line to start it in IDS mode.  The basic command is: sudo snort -i 192.168.2.100 -c /etc/snort/snort.conf 3. Snort will start running and analyze network traffic based on the configured rules. |
| **Shutdown**:   1. Launch a Terminal window on your Linux system. 2. Before shutting down Snort, it's essential to identify any running Snort processes. To do this, run the following command in the Terminal: ps aux | grep snort 3. From the list of running processes, identify the process ID (PID) of the Snort process you wish to shut down. The PID is the number displayed in the second column of the output. 4. send a termination signal to initiate the shutdown. Use the following command: sudo kill 12345 (Where 12345 is the PID of the snort process. |

|  |  |
| --- | --- |
| Anti-virus/Malware | |
| **Sophos (Windows Server)** | **Start-up**:   1. Log in to the Windows 2022 AD Server once the system has fully booted up 2. Locate the Sophos icon in the **‘Start’** menu or system tray of the Windows taskbar.  It appears as a blue shield with a white "S" symbol. 3. Right-click on the Sophos icon to open the context menu. 4. From the context menu, select "Open Sophos Endpoint Security and Control" or a similar option that allows you to access the Sophos security software. 5. The Sophos Endpoint Security and Control console will open, displaying the main interface of the software. 6. Check if the Sophos software shows a "**Running**" or "**Active**" status. If it does, the software is already running and providing protection. If not, continue with the next step. 7. Within the Sophos Endpoint Security and Control console, there should be an option or button to start the software. It may be labeled as "**Start**," "**Enable**," or something similar. Click on it to initiate the start of the Sophos security software. 8. Give the Sophos software a few moments to start up and initialize its components.  The status should change to "**Running**" or "**Active**" once it is fully operational. 9. Check the Sophos icon in the system tray again. It should display an indicator or tooltip confirming that the software is running and providing protection. |
| To properly **shut down** the Sophos security software, follow these instructions:   1. Locate the Sophos icon in the system tray of the Windows taskbar. It appears as a blue shield with a white "S" symbol. 2. Right-click on the Sophos icon to open the context menu. 3. From the context menu, select "**Open Sophos Endpoint Security and Control**" or a similar option that allows you to access the Sophos security software. 4. The Sophos Endpoint Security and Control console will open, displaying the main interface of the software. 5. Within the Sophos console, locate the "**Shutdown**" or "**Stop**" option. This option may be found in the main interface, settings, or preferences. 6. Click on the "**Shutdown**" or "**Stop**" option to initiate the shutdown process for the Sophos security software. 7. A confirmation prompt may appear asking you to confirm the shutdown action. Review the information and click "**Yes**" or "**OK**" to proceed with the shutdown. 8. The Sophos security software will initiate the shutdown process. It may take a few moments to complete the shutdown and deactivate its components. 9. Check the Sophos icon in the system tray again. It should no longer display any active indicators or tooltips, indicating that the software has been successfully shut down. |
| **Sophos Intercept X (Linux Web Server)** | To **start** the Sophos Intercept X antivirus/malware software, follow these instructions:   1. Log in to the Linux 2 web server, once the system has fully booted. 2. Open a terminal to access the command line interface of the Linux server. 3. Run the following command to start the Sophos Intercept X service:   sudo /opt/sophos-av/bin/savdctl start  This command starts the Sophos Intercept X service on the Linux server.   1. Give the Sophos Intercept X service a few moments to start up and initialize its components. You can monitor the progress by checking the terminal or observing any relevant logs. 2. Once the service has started successfully, you can verify its status by running the following command:   sudo /opt/sophos-av/bin/savdstatus   1. This command will display the current status of the Sophos Intercept X service and confirm that it is running. 2. To ensure that the Sophos Intercept X software is actively protecting your Linux 2 web server, you can check the real-time protection status. |
| To **shut down** the Sophos Intercept X anti-virus/malware software, follow these instructions:   1. Open a terminal to access the command line interface of the Linux server. 2. Run the following command to stop the Sophos Intercept X service: sudo /opt/sophos-av/bin/savdctl stop   This command stops the Sophos Intercept X service on the Linux server.   1. Give the Sophos Intercept X service a few moments to shut down and deactivate its components. You can monitor the progress by observing any relevant logs. 2. You can confirm that the Sophos Intercept X service has stopped by running the following command: sudo /opt/sophos-av/bin/savdstatus   This command will display the current status of the Sophos Intercept X service. Ensure that it shows as stopped or inactive.   1. Optionally, you may also want to disable the automatic startup of the Sophos Intercept X service on system boot. To disable automatic startup, run the following command:   sudo /opt/sophos-av/bin/savdctl disable  This command disables the automatic startup of the Sophos Intercept X service. |

|  |  |
| --- | --- |
| Log Monitoring and Analysis | |
| **Splunk (Windows Server)** | **Start-up**:   1. Log in to the Windows AD 2022 server 2. **To open the Splunk application:**  Locate the Splunk application shortcut in the windows ‘**Start**’ menu. **OR** navigate to the installation directory, by default, Splunk is installed in "C:\Program Files\Splunk" or "C:\Program Files (x86)\Splunk" on a Windows server. Double-click on the Splunk executable file, typically named "splunk.exe," to open the application. 3. **Wait for Splunk to start:**  After launching Splunk, the application will initialize and start its services. This process may take a few moments. 4. **Access Splunk Web Interface:**  Once Splunk has finished starting up, open a web browser on the Windows server.  Enter the following URL in the address bar: "**http://localhost:8000**".  If you are accessing Splunk from a different machine, replace "localhost" with the IP address or hostname of the server running Splunk. 5. **Log in to Splunk:** Using an administrator account, enter the username and password in the respective fields on the login page.  Click the "**Sign In**" button to log in to the Splunk web interface. 6. **Explore the Splunk web interface:** Once logged in, you will be presented with the Splunk web interface, also known as the Splunk Home.  This interface provides access to various features and functionalities of Splunk, including data ingestion, searching, and visualizations. |
| **To shut down Splunk:**   1. Access the Splunk web interface using a web browser. 2. Log in to the Splunk web interface with your administrator credentials. 3. Navigate to the Settings menu. 4. Click on "Server Controls" under the "System" section. 5. Click the "Restart" or "Shutdown" button. 6. Confirm the restart or shutdown action. 7. Wait for Splunk to complete the shutdown process. 8. Verify that Splunk has shut down successfully. |
| **Splunk (Linux Web Server)** | **Start-up**:   1. Log in to your Linux 2 system using the appropriate credentials. 2. Open a terminal on the Linux 2 system. 3. Navigate to the directory where Splunk is installed.  By default, Splunk is installed in the "**/opt/splunk**" directory.   cd /opt/splunk   1. Start Splunk by running the following command:   ./bin/splunk start  This command will start the Splunk server and its associated services.   1. **Wait for Splunk to start**:  The startup process may take a few moments, and you will see startup messages in the terminal. 2. Once Splunk has started successfully, it will display a message indicating that the web interface is available. 3. Open a web browser on your local machine. 4. Enter the URL "**http://127.0.0.1:8000**" in the address bar of the web browser. 5. The Splunk web interface will appear, allowing you to log in and access the various features and functionalities of Splunk 6. Note: If you are accessing Splunk from a remote machine, replace "127.0.0.1" with the IP address or hostname of the Linux 2 system. |
| **To shut down Splunk**   1. Open a terminal or SSH into the Linux 2 system. 2. Navigate to the directory where Splunk is installed.   cd /opt/splunk   1. Stop Splunk by running the following command:   ./bin/splunk stop  This command will initiate the shutdown process for Splunk.   1. Wait for Splunk to complete the shutdown process.  You will see messages in the terminal indicating the progress of the shutdown. 2. Once Splunk has shut down successfully, you will see a message indicating the successful shutdown.   Stopping Splunk...  Splunk stopped. |

|  |  |
| --- | --- |
| Real-time Monitoring | |
| **Wireshark (Windows Server)** | **Start-up**:   1. Ensure the windows server is on and operating as expected. 2. From the start menu locate wireshark and run open the program 3. Once Wireshark is launched, you will see a window with various network interfaces listed. 4. Select the interface you want to capture packets from and click the "Start" button (green shark fin icon) in the toolbar. Wireshark will start capturing network traffic on the selected interface 5. As packets are captured, you can view and analyze them in real-time using the different panels and tools available in the Wireshark window |
| **Shutdown**:   1. If you currently have the Wireshark Capture window open, click on the "Stop" button (a red square) in the toolbar to stop capturing packets. 2. Locate the main Wireshark application window and click on the "X" button in the upper-right corner to close it. This action will terminate the Wireshark program. 3. In some cases Wireshark may continue in the background. To ensure Wireshark is completely shut down, follow these steps: 4. Press the Ctrl + Shift + Esc keys simultaneously to open the Task Manager. 5. In the Task Manager window, switch to the "Processes" tab. 6. Look for any processes related to Wireshark, such as "wireshark.exe" or "dumpcap.exe". 7. Right-click on each Wireshark process and select "End Task" to terminate it. 8. Close the Task Manager window. |
| **Wireshark (Linux Web Server)** | **Start-up**:   1. Open a terminal on your Linux system 2. Run Wireshark with the command-line to start: wireshark 3. In the Wireshark user interface, you can select the network interface you want to capture traffic from. 4. To start capturing, click on the desired interface, then click the "Start" button (a green shark fin icon). Wireshark will begin capturing network packets on the selected interface. |
| **Shutdown**:   1. Launch a Terminal window on your Linux system. 2. Identify the process ID (PID) of the Wireshark process, by, execute the following command in the terminal ps aux | grep wireshark. 3. The output will include a column labeled "PID" that displays the process ID number. 4. Once you have identified the PID of the Wireshark process, you can terminate it by running the following command: sudo kill <PID> 5. You can confirm that the Wireshark process is no longer running by executing the ps aux | grep wireshark command again. |

|  |
| --- |
| Regular Maintenance Activities with Schedule: |

|  |  |
| --- | --- |
| Windows AD Server | |
| **Patch Management** | Install Windows updates regularly, following the recommended patching schedule (e.g., monthly Patch Tuesday). |
| **Anti-virus Updates** | Ensure the Sophos anti-virus software is configured to update virus definitions automatically, preferably on a daily basis. |
| **Firewall Rule Review** | Periodically review and update firewall rules to ensure proper security measures |
| **Log Analysis** | Regularly monitor and analyze logs using Splunk to identify potential security incidents or system issues |
| **Backup Verification** | Periodically test and verify the integrity of system and data backups |

|  |  |
| --- | --- |
| Linux Web Server | |
| **Patch Management** | Install Windows updates regularly, following the recommended patching schedule (e.g., monthly Patch Tuesday). |
| **Anti-virus Updates** | Ensure the Sophos anti-virus software is configured to update virus definitions automatically, preferably on a daily basis. |
| **Firewall Rule Review** | Periodically review and update firewall rules to ensure proper security measures |
| **Log Analysis** | Regularly monitor and analyze logs using Splunk to identify potential security incidents or system issues |
| **Backup Verification** | Periodically test and verify the integrity of system and data backups |

|  |
| --- |
| Support Processes and Documentation |

|  |  |
| --- | --- |
| **Incident Response:** | Document the process for handling security incidents, including steps to identify, contain, eradicate, and recover from any security breaches or anomalies |
| **Change Management** | Establish a change management process to document and track any modifications or updates made to the infrastructure, including security software configurations, firewall rules, and system changes |

|  |
| --- |
| User Access Management: |

|  |  |
| --- | --- |
| Processes of Access Management | |
| **User Provisioning:**   * **Creating user accounts**: When a new user needs access to the system, an administrator creates a user account with appropriate permissions and access rights. * **Assigning roles and permissions**: Based on the user's job responsibilities and requirements, the administrator assigns appropriate roles and permissions to the user account.   **User Authentication:**   * **User authentication methods**: Implement authentication methods such as passwords, multi-factor authentication (MFA), or biometrics to verify the identity of users during login. * **Password policies**: Enforce strong password policies, including password complexity requirements, expiration, and account lockout settings. * **Implementing MFA**: Enable MFA for users to add an extra layer of security by requiring an additional form of authentication, such as a verification code sent to their mobile device.   **User Authorization:**   * **Role-based access control (RBAC):** Implement RBAC to assign users to specific roles with predefined permissions, allowing them to access only the resources necessary for their job functions. * **Access control lists (ACLs):** Use ACLs to define specific permissions for individual users or groups on files, folders, or network resources. * **Regular access reviews**: Conduct periodic access reviews to ensure that users still require the assigned access rights and permissions. Remove or modify access as necessary.   **User Account Management:**   * **Modifying user accounts:** Update user account information when there are changes in job roles, responsibilities, or personal details. Modify permissions or access rights accordingly. * **Disabling user accounts**: Disable user accounts promptly when users leave the organization, change roles, or no longer require system access. * **Account lockout policies**: Implement account lockout policies to prevent unauthorized access attempts by locking user accounts after multiple failed login attempts. | |
| Managing User Accounts | |
| **Creating user accounts** | Windows Server: In the Windows Server environment, an administrator can create user accounts through the Active Directory Users and Computers management console or using PowerShell commands.  Linux Web Server: On a Linux web server, an administrator can create user accounts using the "useradd" command or through user management tools like "useradd" or "adduser." |
| **Modifying user accounts** | Windows Server: To modify user accounts on Windows Server, an administrator can use the Active Directory Users and Computers management console or PowerShell commands to update user attributes such as username, password, group membership, and permissions.  Linux Web Server: On a Linux web server, an administrator can modify user accounts by using commands like "usermod" or by editing user configuration files manually. |
| **Disabling user accounts** | Windows Server: In the Windows Server environment, an administrator can disable user accounts through the Active Directory Users and Computers management console or using PowerShell commands. Disabling an account restricts user access while retaining account information.  Linux Web Server: On a Linux web server, an administrator can disable user accounts by modifying the account status in the user configuration files or using commands like "usermod" or "passwd." |
| **Managing Azure AD 2FA** | Azure Active Directory (AD) supports multi-factor authentication (MFA) to enhance user account security. Administrators can enable and manage MFA settings for Azure AD users through the Azure portal or PowerShell commands. |
| **AD Windows Server** | To enable Azure AD 2FA, administrators can navigate to the Azure portal, select the Azure AD directory, go to "Security," and configure MFA settings. This may include options like SMS, phone call, or mobile app verification |

|  |
| --- |
| Support Contacts: |

Maintain a list of support contacts, including vendor support for each security software, operating system support, and any internal IT support personnel responsible for the infrastructure.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Organisation** | **Contact details (Email / Phone)** |
| Mauricio Guerra | System Administrator | SecureNET | mguerra@securenet.com |
| Shaun Heywood | Security Analyst | SecureNET | sheywood@securenet.com |
| Vendor Support | Sophos Firewall | Sophos | support@sophos.com |
| Vendor Support | Sophos Intercept X | Sophos | support@sophos.com |
| Vendor Support | Snort IDS | Cisco | support@cisco.com |
| Vendor Support | Splunk Log Management | Splunk | support@splunk.com |
| IT Support | Internal IT Department | OzCazual | helpdesk@ozcazual.com |

This operational and support documentation is periodically reviewed, updated, and communicated to relevant personnel to ensure the continued management and security of the revised infrastructure.